University of South-Eastern Norway

Access Security in Mobile Systems

Security Evolution over 50 Years

Geir M. Køien

A Brief Summary of the Mobil Security Evolution

The Generations

1G: ≈1980 - where it started (well, almost)
2G: ≈1990 – going digital (a la ISDN)
3G: ≈2000 – going IP (but not exclusively)
4G: ≈2010 – going all-IP
5G: ≈2020 – going all-virtual (software)
6G: ≈2030 – going all-political

My background:

- Worked with NMT while at Ericsson
- Worked with GSM, UMTS and LTE while at Telenor R&D
- Telenor delegate to 3GPP SA3 for 10+ years
- Rapporteur for NDS/IP specs
- Been part of the 1G → 5G evolution

10 Year Cycle

Time

- The 10 years cycle of the generations
- From dedicated HW to SW all-over (even the SIM)
- From national coverage to global coverage
- From being an auxiliary service to being a primary critical infrastructure

Time changes everything!

Assets and Threats

- Initially:
  - To get access was costly.
  - Metering rates were high. Metering fraud was real.
- Today:
  - Fixed rates, bulk data.
  - Nobody cares about a few Gb's anymore.
  - But scalability matters!!
- Value has moved up in the stack
  - From metering (low-level access, link layer'ish)
  - To services (high-level)

(operator)

The Basic System Architecture

Subscribers

- Subscriber Identity Module (SIM) – tamper resistant
- Mobile Equipment (ME)

Components of the mobile station

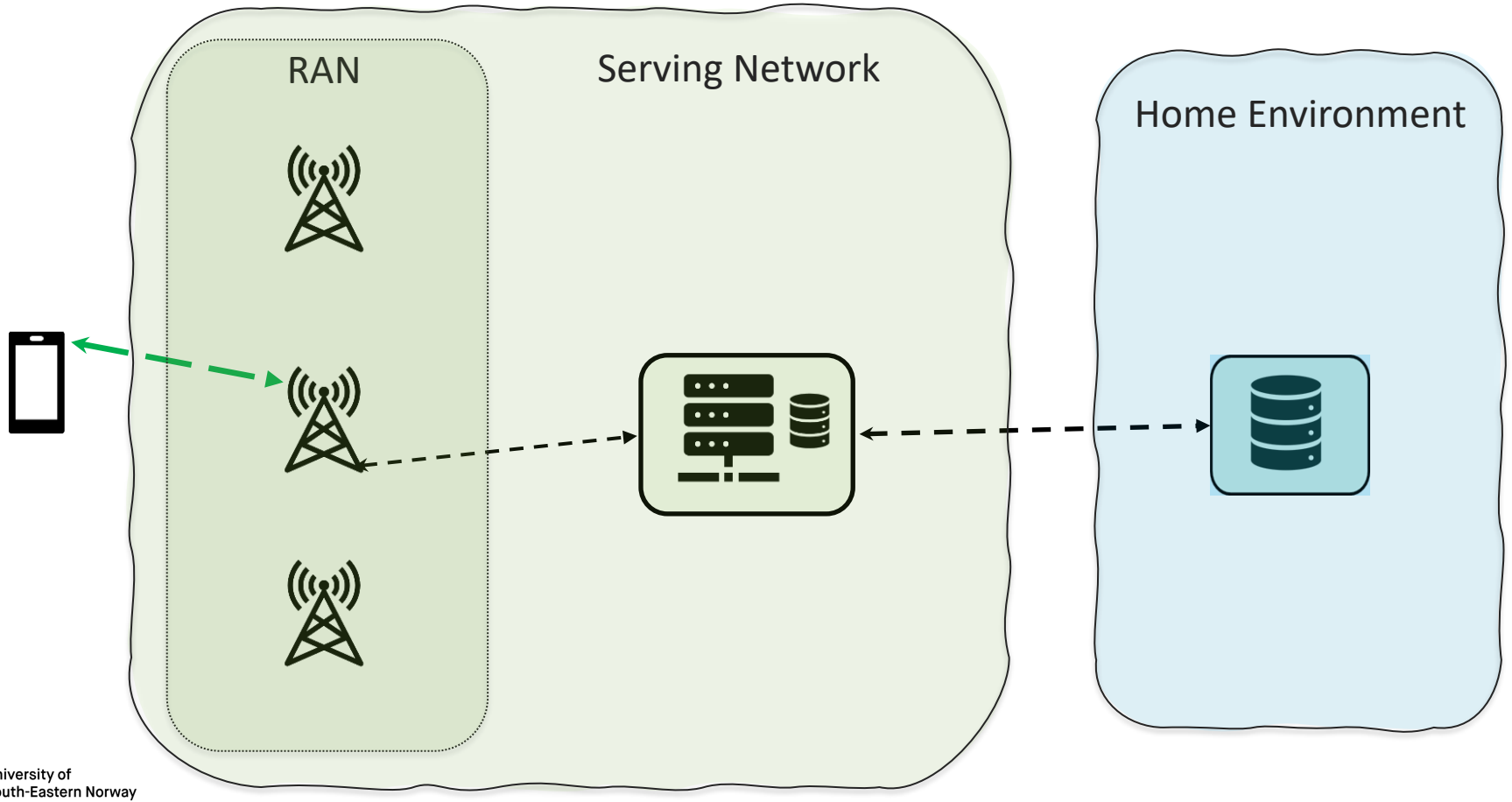
Subscriptions

- SIM is issued by the home operator
- SIM contains subscription credentials (and authentication algorithms)
- ME contains over-the-air encryption algorithms

Roaming

- “Roaming agreements” between network operators
- Subscriber can move between networks (if permitted)

The Basic System Architecture



Public Land Mobil Networks (PLMNs)

"Home" networks: HPLMN

- Home Environment (HE): subscription data, location data and subscription credentials
- May have a serving network

The "Serving network (SN)":

- Core Network (CN): Servers, local databases, etc.
- Radio Access Networks (RANs): with base-stations and controllers

"Visited" networks: VPLMN

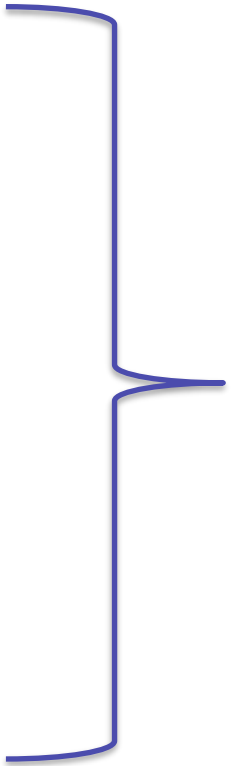
- A "foreign" network with roaming agreement with the home operator
- Has SN functionality

Protection of Assets

Subscriber Perspective
- Protection against eavesdropping (over-the-air)
- Avoiding being cheated (fraud)

The networks
- Getting paid
- Being perceived to be trustworthy
- Being able to trust other networks

Society (regulations, …)
- Availability of affordable critical services
- Fairness (competition)



Different perspectives
Different assets

Different threats
Different priorities

Protection of Assets

Subscriber Perspective
- Protection against eavesdropping (over-the-air)
- Avoiding being cheated (fraud)

The networks
- Getting paid
- Being perceived to be trustworthy
- Being able to trust other networks

Society (regulations, …)
- Availability of affordable critical services
- Fairness (competition)

Key Question:

Who Decides?

Security Goals (since 2G) – Subscriber view

Data Confidentiality
- Protection against eavesdropping (over-the-air)

Identity- and Location Confidentiality
- Avoid tracking, etc.
- Solved in 5G with “SUCI”

Authentication and Key Agreement (AKA)
- Establishing a security context

Be Aware:
To the operators, only threats that scale are important!

AKA Protocols

- Network initiated, only the SIM gets challenged
- (Pseudo-)Random challenge and MAC-based Response (with pre-shared auth.secret)
- Gradually moving from one-way towards mutual authentication
- Pre-shared secret authentication key (K) at SIM and HPLMN (128-bit)

1.	NMT	SIS	No keys derived
2.	GSM	AKA	One 64-bit session key derived
3.	UMTS	AKA	2 x 128-bit session keys derived
4.	LTE	AKA	1x 256-bit key-deriving key (for a key hierarchy)
5.	5G	AKA	a lot like 4G, but with a different key hierarchy
6.	6G	AKA	(quantum-safe design?)

"key" needs determined by radio access design

The actual systems

The Early Days (1G/NMT)

NMT (450 og 900)

- 25 kHz analogue speech channel
- Digital access signaling (“frames”)
- Base stations directly connected to a switch (MTX)

Security Measures

- Originally:
  - 3 digit “password” (transmitted in cleartext)
  - Eavesdropping problem – speech in clear
- Then there was fraud…
  - NMT SIS (a separate hw module)
  - Challenge-Response protocol to authenticate subscribers

2G background

- Designed during late 1980ies
- Smartcards and crypto-HW in **MS** was a bold step
- National incumbent operators in Europe
- Very few “digital” threats at the time
- **But there were 1G lessons…**

Going All-Digital (2G/GSM)

GSM is all-digital

- Primarily a circuit-switched (narrowband) system
- Re-uses ISDN designs and is very much inspired by ISDN
- Speech (and data) is all-digital → encryption (over-the-air) is possible
- GSM AKA protocol to set up a security context

Networks

- SS7-based signaling (with “modern” extensions like TCAP)
- Data channel were 64 kbps (belonging to a 2 Mbps set)
- There was absolutely no security in the SS7 signaling networks!

GSM AKA protocol – setting up a security context

Basic credentials

- On SIM and in AuC (home network):
  - IMSI – the subscription identifier
  - Ki – the secret authentication key (128-bit)

```
Triplet:
 RAND: 128-bit
 SRES: 32-bit
 Kc:   64-bit
```

Challenge-Response

- The HPLMN issues Authentication Sets (triplets) to the VPLMN
- The VLR/SGSN *challenges* the SIM with a RANDom challenge
- The SIM *responds* with a Signed RESponse message

A3/A8 algorithms

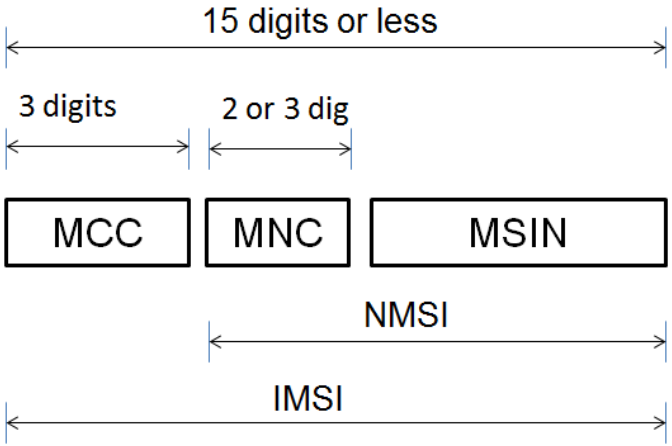
- A3/A8 are interfaces
- Default algorithm (COMP128) was very weak (and in use…)
- Kc was initially limited to 54 significant bits

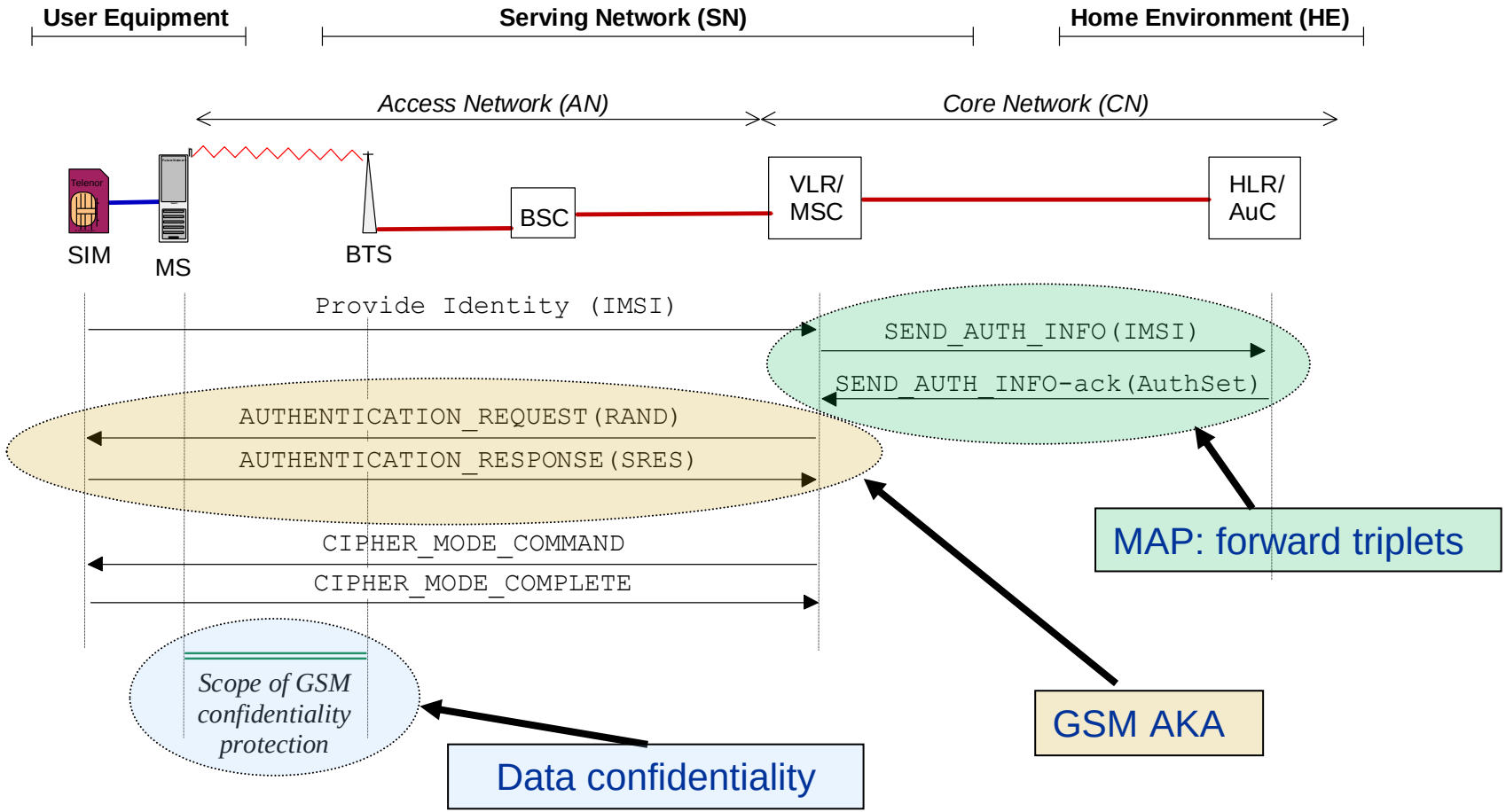
```
A38(Ki,RAND) → SRES,Kc
```

IMSI

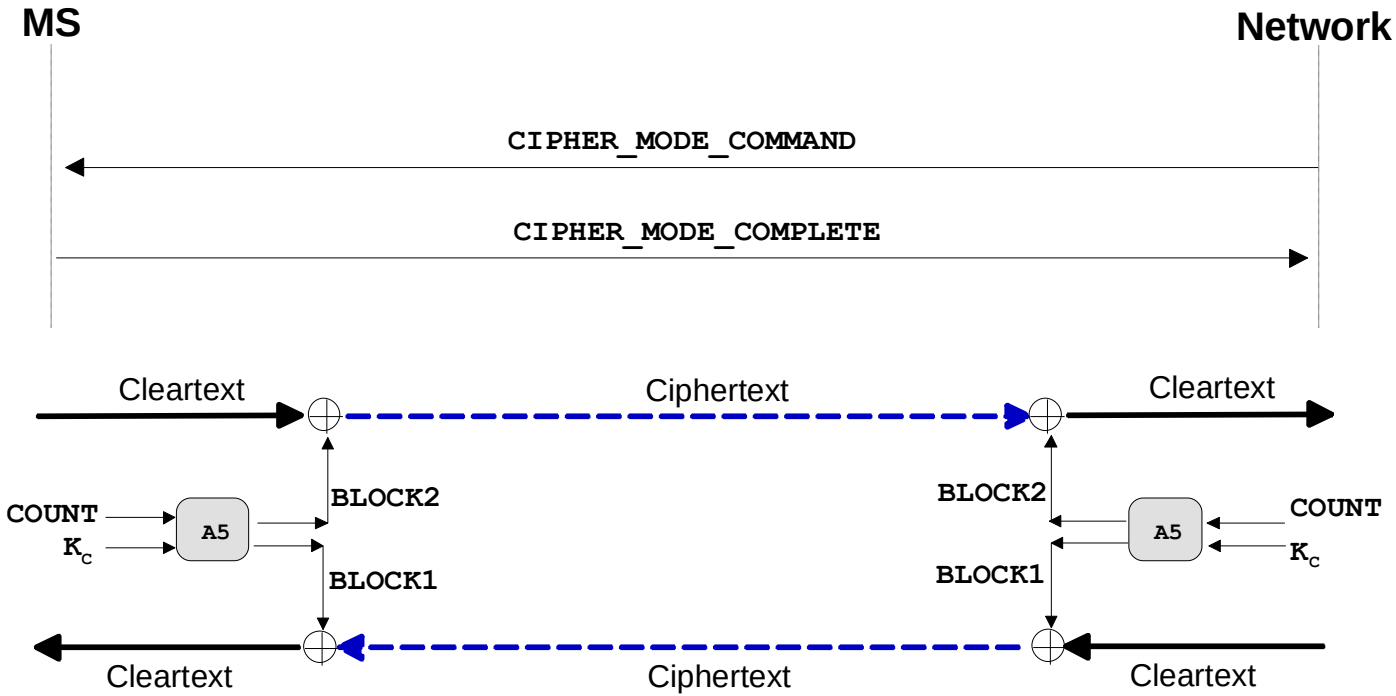
International Mobile Subscriber Identity

- Based on ITU-T E.212 recommendation
  - Mobile Country Code (MCC): 3 digits (decided by ITU)
  - Mobile Network Code (MNC): 2 (or 3) digits (decided by national authorities)
  - Mobile Subscription Identification Number (MSIN): 9 (or 10) digits (decided by the operator)




User Equipment
Serving Network (SN)
Home Environment (HE)
Access Network (AN)
Core Network (CN)
SIM
MS
BTS
BSC
VLR/
MSC
HLR/
AuC
Provide Identity (IMSI)
SEND_AUTH_INFO(IMSI)
SEND_AUTH_INFO-ack(AuthSet)
AUTHENTICATION_REQUEST(RAND)
AUTHENTICATION_RESPONSE(SRES)
CIPHER_MODE_COMMAND
CIPHER_MODE_COMPLETE
Scope of GSM confidentiality protection
MAP: forward triplets
GSM AKA
Data confidentiality

Encryption in GSM – Always network initiated



Note:

A5 is a family of stream ciphers.

- A5/1 – the original
- A5/2 – a weakened version
- A5/3 – the current one
- A5/4 – a 128-bit version

Note:

- The BLOCK is 114-bits
- COUNT is a frame-number
- Will loop after ≈ 3.5 hours
- Must run AKA to update Kc

2G security: Was it sufficient?

- No network security
- Thus: Required complete trust in anybody with access to SS7-signaling

- No verification of the network whatsoever – thus were born the “false-basestation” problem
- Smartcards of varying pedigree
- COMP128 was abysmally weak
- A5/1 was originally limited to 54 bits
- No keybinding
- No restrictions on key re-use

- AKA was optional!
- Use of A5 was also optional

GSM security was a huge success!

3G background

- Designed during late 1990ies
- **64-bit security was seen as inadequate**

- IMT-2000 was the high-level functional definition
- ETSI proposed the UMTS system (based on GSM, but with a UTRAN)
- There were two main 3G system (but UMTS “won” in the end)

- To provide broadband’ish IP-connectivity was important
- But it was also important to be **backwards compatible** with ISDN/SS7 systems

Supporting IP (3G/UMTS)

UMTS – all digital, IP-support, yet still circuits-switched too

- UMTS AKA based on Rijndael and KASUMI cipher (3G-SNOW/AES later)
- UTRAN support (and GERAN (GSM+GPRS))
- Marked the beginning of the smartphone age

Networks

- SS7-part still not protected
- IP part (GTP, DIAMETER, …) *could* be protected (NDS/IP, based on IPsec)….

Threats

- Changed threat landscape (bigger assets *and* more threat actors)
- Many more operator, even less security…

UMTS Security Architecture

- **3G - UMTS**
  - Security analysis and requirements doc (TS 21.133)
  - A separate “Objectives and Principles” doc (TS 33.120)
  - A security architecture (TS 33.102)
  - Cryptographic requirements(TS 33.105)
  - Public spec of all crypto (sort of)
    - KAUSUMI TS 35.201 – TS 35.204
      - Later also SNOW-3G: TS 33.215 – TS 33.218
    - AKA algo: MILENAGE TS 35.205 – TS 35.208 (based on Rijndael)

UMTS specified use of 128-bit algorithms before they were allowed

- **Security goals (TS 33.120)**
  - Security elements within GSM and other second-generation systems that have proved to be **needed** and **robust** shall be adopted for 3G security.
  - 3G security will address and correct real and perceived weaknesses in second generation systems.
  - 3G security will offer new security features and will secure new services offered by 3G.

UMTS, MILENAGE

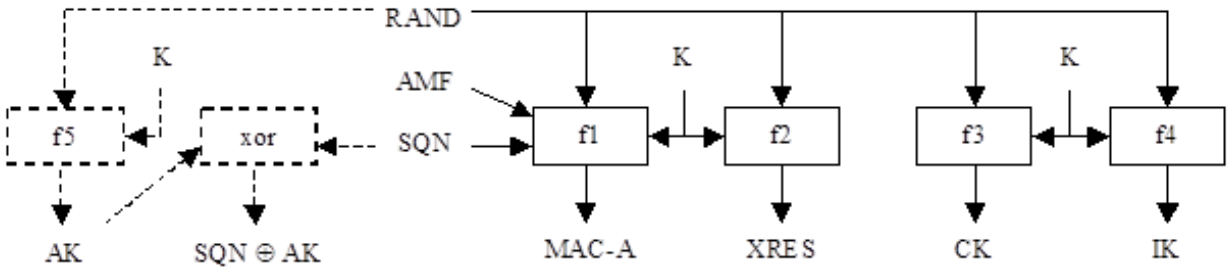
AKA algo: **MILENAGE**, in TS 35.205 – TS 35.208 (based on Rijndael)

- **Authentication Vector (AV):**
  - RAND: 128-bit
  - RES: 64-bit (usually)
  - CK,IK: 128-bit session keys
  - AUTN: Authentication Token

(instead of triplets)

Challenge: **RAND,AUTN**

Response: **RES**

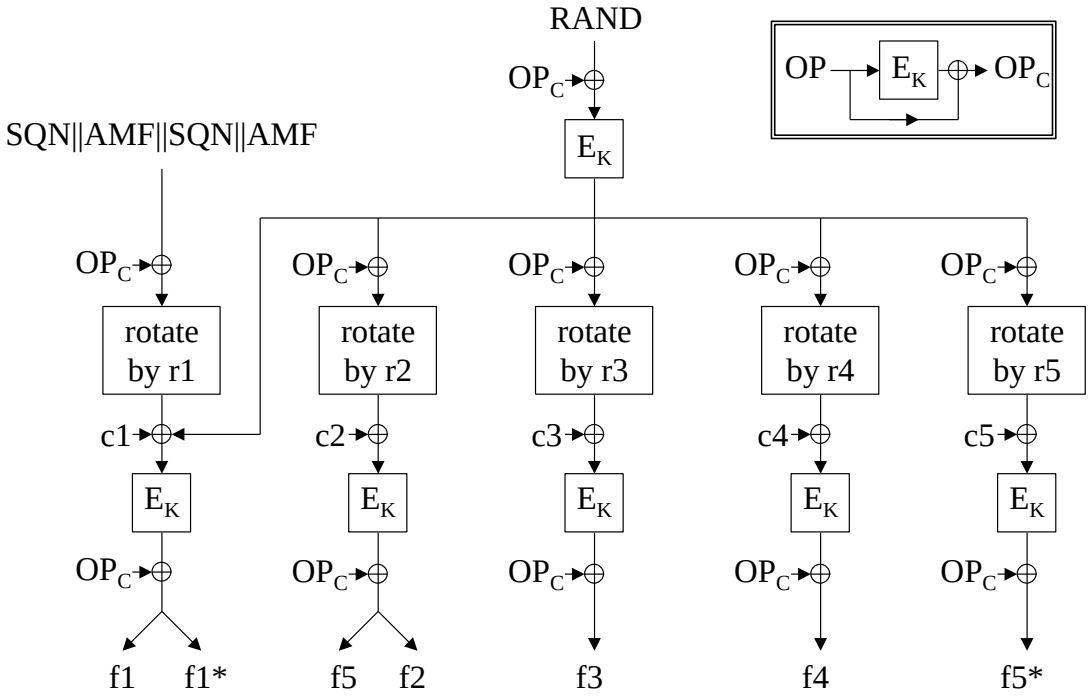


AUTN = SQN [⊖ AK] || AMF || MAC-A
Quintet = (RAND, XRES, CK, IK, AUTN)

MILENAGE – The f-functions

AKA algo: MILENAGE TS 35.205 – TS 35.208 (based on Rijndael)

- Clever **OP_C** construct to conceal the operator configuration (**OP**) parameter
- **E** is Rijndael

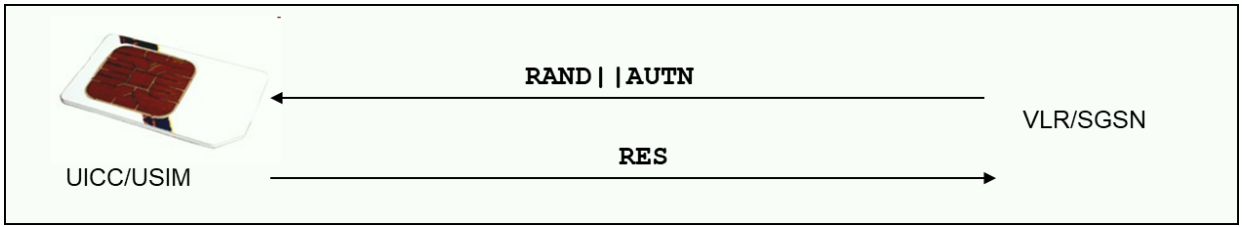


UMTS AKA protocol

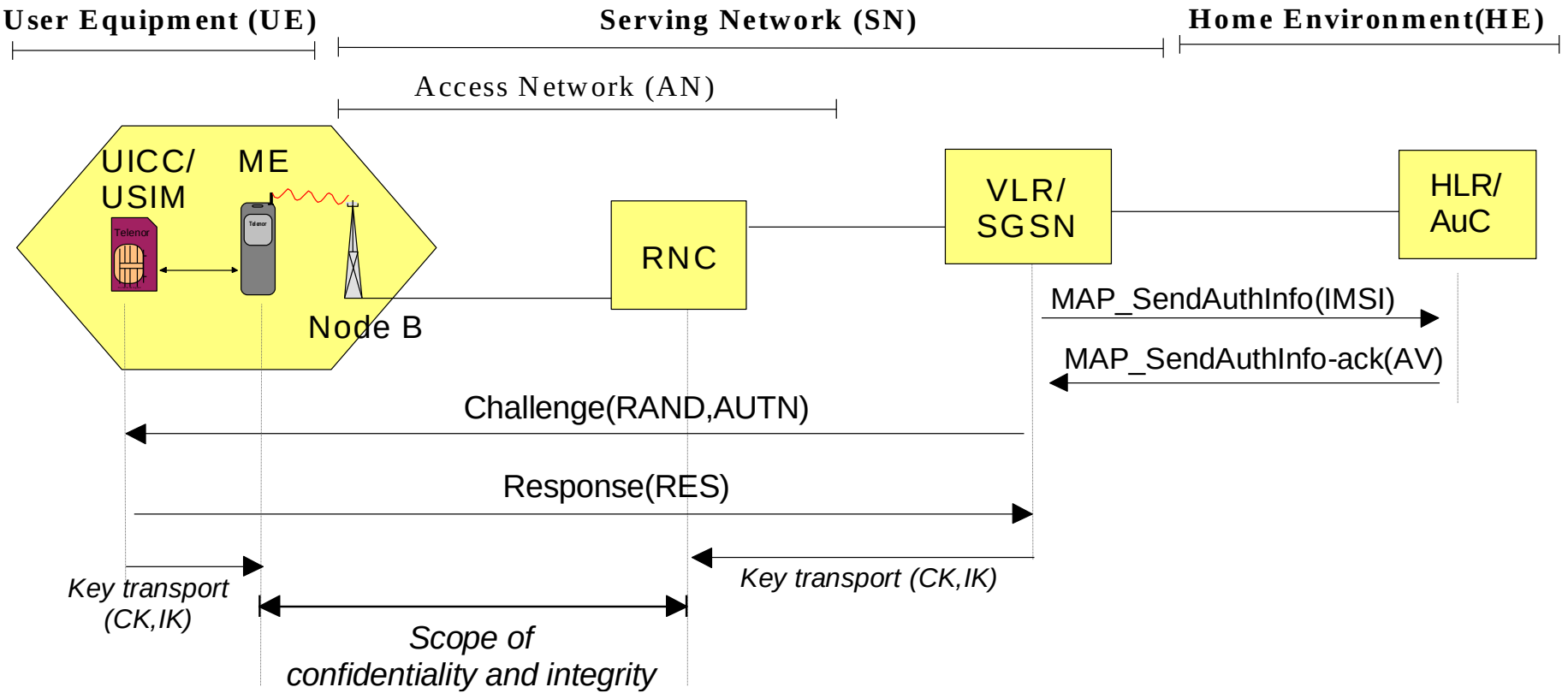
- **Preliminary step (forwarding of AVs)**
  - Yes, the **AV**s are forwarded to the VPLMN (blind trust….)

NOTE:
SIM is called USIM in UMTS.
USIM is software on the smartcard.

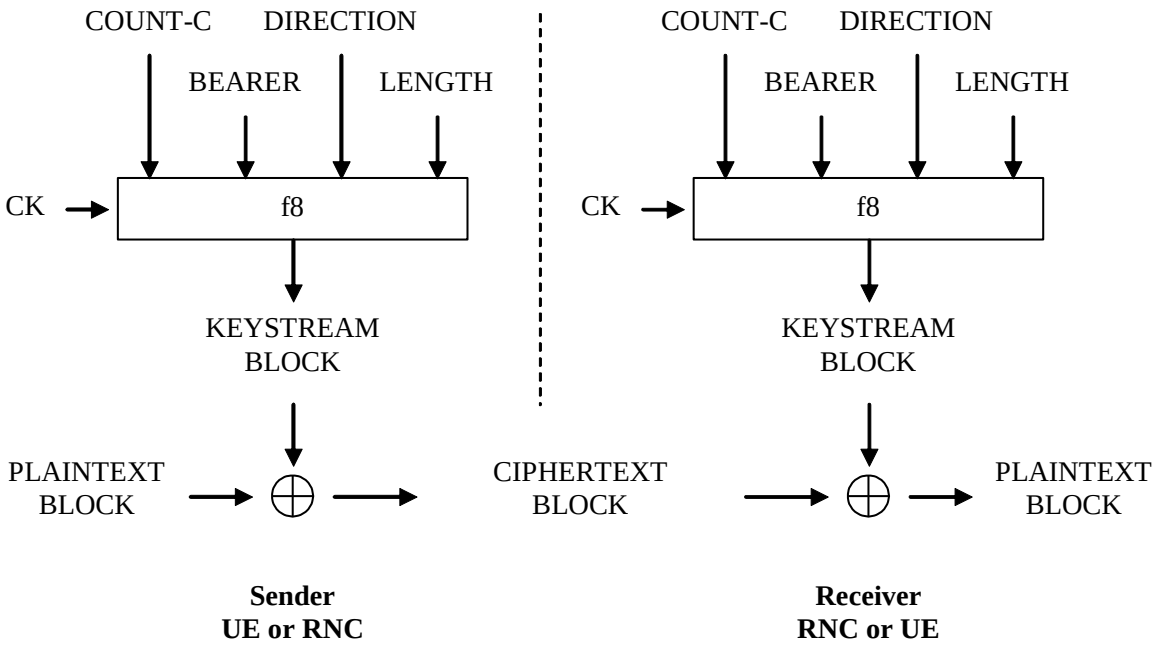
- **UMTS AKA**
  - **IMSI** and the 128-bit Ki (now called **K**) is still the basis
  - UMTS provides authentication of the challenge (so we know it originated with the HE)
  - There is a **sequence number (SQN)** scheme (timeliness…)
  - Larger **RES** (usually 64-bit now)
  - Two 128-bit session keys: **CK** and **IK**



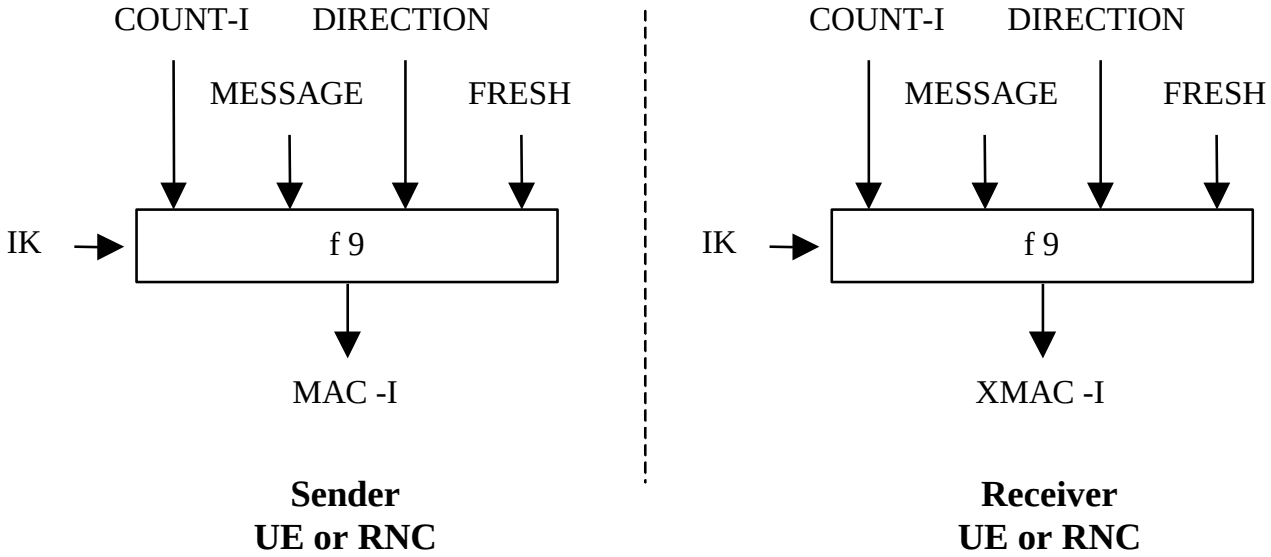
AUTN = SQN⊕AK||AMF||MAC-A


User Equipment (UE)
Serving Network (SN)
Home Environment(HE)
Access Network (AN)
UICC/
USIM
ME
Telenor
Telenor
Node B
RNC
VLR/
SGSN
HLR/
AuC
MAP_SendAuthInfo(IMSI)
MAP_SendAuthInfo-ack(AV)
Challenge(RAND,AUTN)
Response(RES)
Key transport
(CK,IK)
Key transport (CK,IK)
Scope of
confidentiality and integrity

UMTS f8-function



UMTS f9-function (only for signaling)



3G security: Was it sufficient?

- No network security in practice (though NDS/IP was available)
- Roaming networks (GRX/IPX) never focused on security
- Thus: Required trust in other networks

} "Attack" tools exists

- No real verification of the network – "false-basestation" problem remains
- UICC/USIMs of varying pedigree
- Backwards compatibility with 2G (ouch!!)
- …and 2G could routinely be hacked by now…
- No key-binding
- No real restrictions on key re-use

- AKA was no longer optional!
- But use of f8 included a null cipher option

UMTS security was a success (but with clouds on the horizon)

4G background

- Designed just prior to 2010
- All-IP, Fully embraced IP
- Greenfield 4G does not need SS7 anymore

- Long-Term Evolution (**LTE**) comes in several flavors (no security impact)
- Evolved Packet System (**EPS**) is the design for the core network
- Plane separation (**user plane**, **control plane**)

- AKA protocols is known as EPS AKA

- **Threat Landscape**
  - Mobile phones have become important targets!

All-IP (4G/LTE)

- **Many changes between 3G and 4G system architectures**
- **Over-the-air security(?)**
  - In 2G there was MS-BTS security.
  - In 3G this extended to the RNC
  - In 4G, security is yet again terminated in the basestation (eNodeB)
  - **Non-Access Stratum** (control plane) is encrypted between the MS and the MME

BUT: USIM is retained (→ authentication will thus be UMTS'ish)

- Costly to change **SIM**, so the **UICC/USIM** was retained in **4G**
- Implication: Improvements in 4G must be implemented in the ME

All-IP (4G/LTE)

- **The EPS AKA protocol (**See TS 33.401 for the gory details**)**
  - Similar to UMTS AKA in most respects
  - There is a “separation” bit in the **AMF** now
  - **User side:**
    - **USIM** still sees a “UMTS” challenge and replies with a “UMTS” response
    - **ME** must do the rest
  - **Key Hierarchy**
    - Session keys (**CK,IK**) replaced with *key-deriving key* (called **K_{ASME}**)
    - Re-keying is therefore much easier to do…

All-IP (4G/LTE)

- **The EPS AKA protocol**
  - Still a two-stage protocol (**BAD**)
  - GSM SIM not acceptable (**GOOD**)
  - **IMSI** and **K** is still there (in the 3G USIM)
  - Challenge is “LTE” specific

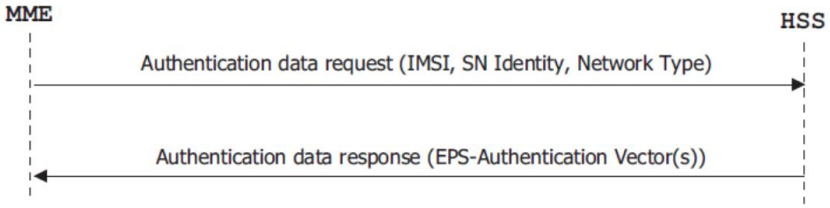


Figure 3.10 Distribution of EPS-AV from HE(HSS) to SN(MME).

  - **The EPS AV:**
    - RAND: 128-bit
    - RES: 64-bit
    - K_{ASME}: 256-bit
    - AUTN (SQN + AMF + MAC-A)

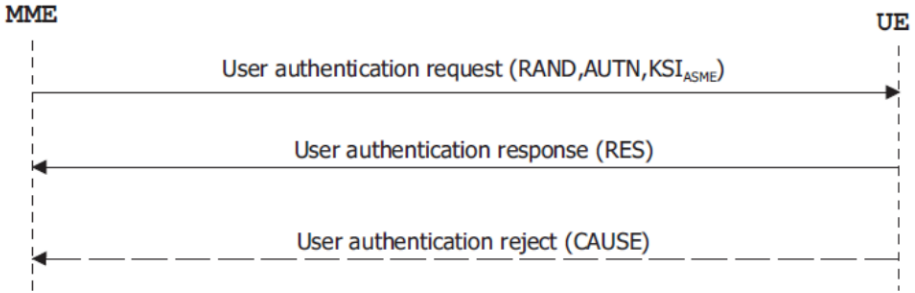
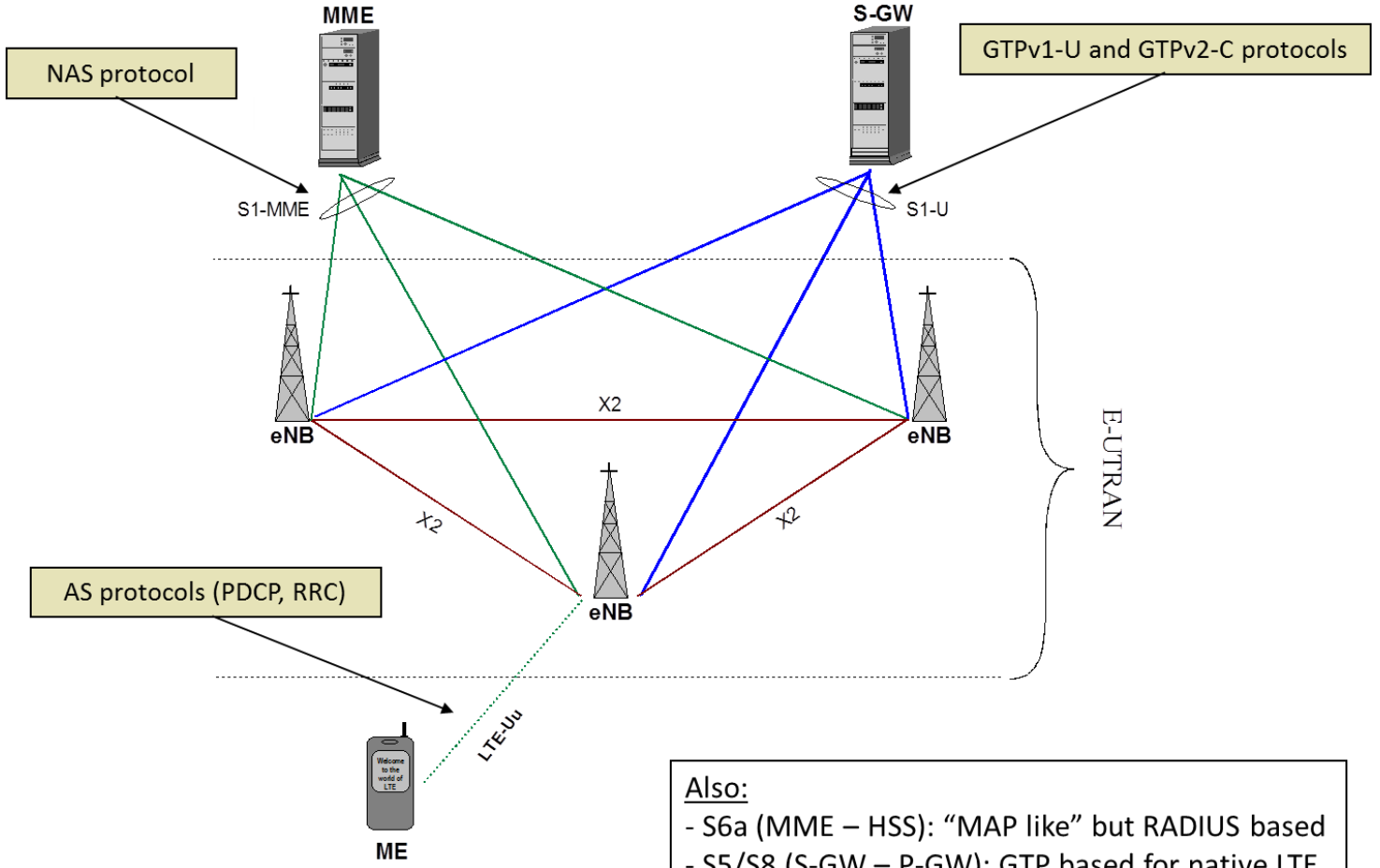


Figure 3.11 EPS authentication.



Also:
- S6a (MME – HSS): "MAP like" but RADIUS based
- S5/S8 (S-GW – P-GW): GTP based for native LTE

All-IP (4G/LTE)

- **The EPS AKA protocol**
  - The authenticated **challenge** is bound to the VPLMN-id
  - But still only indirect mutual authentication (HPLMN – USIM)
  - GSM SIM not permitted (it was permitted in UMTS)

- **Security contexts and Key Hierarchies**
  - EPS Security Context: Established by EPS-AKA
  - NAS Security Context: Established in conjunction with EPS-AKA
  - AS Security Context: Established when needed

  - **K_{ASME}** now is the root of a large key hierarchy
  - Keys are derived from **K_{ASME}**
  - Standardized key deriving algorithm (based on HMAC-SHA-256)
  - Principle: **one key for each use**

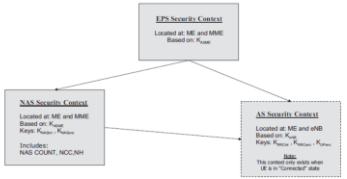


Figure 3.12 EPS context hierarchy.

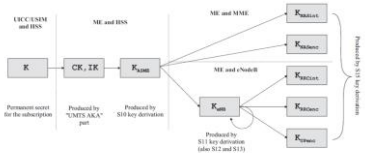


Figure 3.13 EPS key hierarchy.

All-IP (4G/LTE)

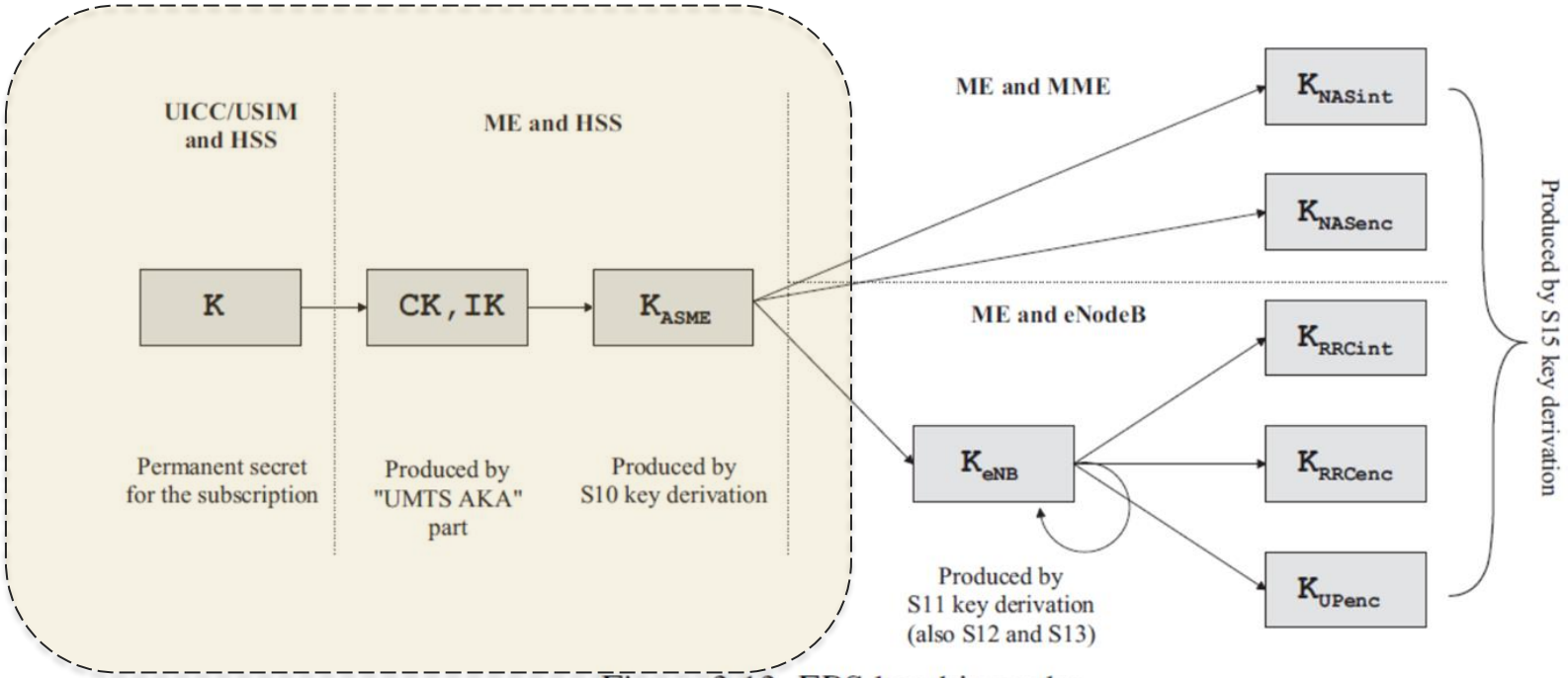


Figure 3.13 EPS key hierarchy.

4G security: Was it sufficient?

- Still no network security in practice
- Roaming networks (GRX/IPX) never focused on security
- Thus: Required trust in other networks
- Critical infrastructure – (operators now need a **blue team**)

Need Zero Trust thinking here

- No real verification of the network elements – "false-basestation" problem remains!!

- UICC/USIMs of varying pedigree

- Use of null cipher option still exists
- Does the end-points measure up?
- **128-bit security is no good if the Apps are bad**

4G security is still a success (if you're the operator)

"Access security" is not enough for the user!

Good enough?

Are we solving the right problem?

What about 5G?

Or 6G?

```
sys.exit(0)
```